ICT Educator Webinar Series

Haiku Cyber Range: Cyber Training for the Masses

October 11, 2019

Table of Contents

[00:00:00]

Welcome

STEVE WRIGHT: Good morning, everybody. Welcome to the ICT Educator Webinar Series. I'm Steve Wright, Statewide Director of the California Community College ICT Sector Team. If you visit our website, you'll see our ten Regional Directors throughout the state and our support team, which includes Nicole Sherman, the producer of this series, and Shawn Monsen, who often brings some extraordinary talent like today's guest.

The series is open access and is provided for the benefit of the California community college faculty, deans, decision makers, department heads, and other related education groups. The series was developed to provide superior IT information with relevance to your campus, so you don't have to go to an expensive conference. You can register each week in advance. Friday at 10 AM, you can just tune in for another exciting session!

Posted Webinars

- Cloudification of the IT Model Curriculum
- 3 Ways Your Campus Can Offer Industry Certification Exams
- Cisco Update: A New Streamlined Certification Program
- Choosing the Right Cyber Activities for Your Campus
- Completing a 4-Year Degree in Cybersecurity Through the CA Community Colleges
- Digital Credentials in the California Community Colleges
- NETLAB+ User Group Webinars: Capture the Flag Competitions, Summer Cyber Camps, and More
- Promoting Community College Programs Through Cyber Competitions
- How WASTC Training Helps ICT Educators Stay Current
- Virtual Labs: Practice Labs in the South Central Coast Region

Here are some of the recent webinars we've had. Each webinar, like this one, is recorded, chapterized in the video, transcribed, along with the PowerPoint presentations and relevant links. Many of our faculty consider this an excellent resource to view at any time after it's recorded.

Upcoming Webinars

- **October 25 –** Save Money on Certifications with CompTIA's Academy Partner Program
- **November 1 –** Cybersecurity Dual Enrollment Pathway at Cypress College
- **November 8 –** Exploring the ICT Disciplines: Which ICT Career is For You?

Coming up in the next few weeks, we have on October 25… I think we skip a week—that's right—because of the big conference. Then, October 25 is CompTIA's Academy Partner Program. November 1, Cybersecurity Dual Enrollment Pathway, and on the 8th, which ICT discipline makes the most sense to you? So, that's some great stuff.

What We'll Cover Today

[00:01:31]

STEVE WRIGHT: Today, we're going to focus on the Haiku Cyber Range for Cybersecurity Training, and I was really intrigued by looking at the bios of both these presenters. I think we have a lot of expertise—kind of an overabundance—in military, business, and just a whole lot going on. I'm kind of wondering about this company and where it's going. So, Justin, maybe you can tell us a little bit more about Sentek and the product that you have. We're really looking forward to it, so go ahead and take it away.

[00:02:09]

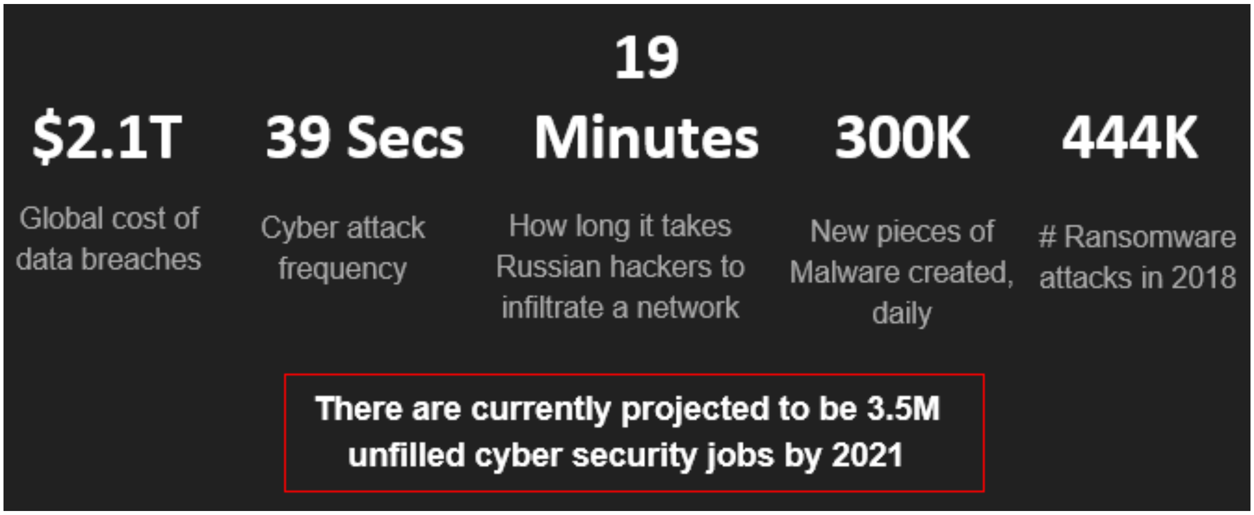
Cyber Training for the Masses

JUSTIN PARKER: Excellent, OK! So, hi, everybody. My name is Justin Parker. I'm a Director here at Sentek Global, and I'm also the Director for the Haiku Cyber Range. Eric Basu, the CEO was planning on joining the call today. Unfortunately, he had some travel issues that occurred at the last minute that basically have him on an airplane at this point in time, but he's very, very interested to see the recording of this, and he'll also be available to answer any follow-up questions and things like that as well.

I've been with Sentek Global now for ten years—I hit it back in August. It was my first job out of the D.O.D. My initial background was actually not in the Cybersecurity realm. I'm an engineer by training—a Systems Engineer and Systems Architect—and through the course of being with Sentek Global, I've moved up from, like I said, just on site, helping out, intelligence surveillance/reconnaissance systems and commanding control systems for various defense partners, to moving into our commercial sector, providing Cybersecurity solutions for commercial customers, and also now overseeing a division within the organization that manages government D.O.D., commercial Cybersecurity services, and now the Haiku Cyber Range.

So, one other thing, too—please feel free to ask questions throughout this presentation and throughout the demo I'm going to give about the Haiku Cyber Range. We're obviously going to have opportunity for questions at the end, too, but you're not going to throw me off my game if you guys interrupt or need some kind of clarification point.

Current State of Global Cybersecurity



$2.1T
Global cost of data breaches

39 Secs
Cyber attack frequency

19 Minutes
How long it takes Russian hackers to infiltrate a network

300K
New pieces of Malware created, daily

444K
Ransomware attacks in 2018

There are currently projected to be 3.5M unfilled cyber security jobs by 2021

[00:03:46]

JUSTIN PARKER: So, the first slide is the very traditional Cybersecurity we're-going-to-scare-the-heck-out-of-you slide, and anybody that's involved in Cybersecurity or has situational awareness knows right now that things are pretty bad.

Working with my customers in the various different government sectors, I'll tell you right now, for every dollar a hacker spends on trying to breach the government and the military and commercial sectors, we're spending about $1,000 right now, and that gets right back to the global cost of data breaches.

I'm not going to go through the laundry list of recent major data breaches that we've had. All you have to do is go through Google News, and you'll probably find one that popped up today. The Cybersecurity attacks are basically nonstop—every 39 seconds is the data that we pulled here, but that's what we can tell.

Everybody is familiar with some state-sponsored hacking that we see going on right now with various countries, and the N.S.A. points out that it usually takes on average a Russian hacker about 19 minutes to infiltrate a network.

Malware and ransomware attacks continue to escalate. I've had several commercial clients that have had the ransomware attacks, and once they've been grabbed, essentially, at the end of the day, we have to start their entire internal networks over again, or they have to pay the ransom tax. It's already too late if that's occurred—there's no putting Pandora back in the box—and that's becoming an incredibly lucrative international crime that continues to only escalate.

The final box there is that by 2021 we anticipate there 3.5 million Cybersecurity jobs available that cannot be filled. I can tell you right now, from an industry perspective, Cybersecurity engineer unemployment is at -5%. So, already we're sitting right now at 5% of the Cybersecurity jobs that are critical to be filled are opened just simply because we have the lack of personnel that can do the job.

So, from an educator standpoint, if you're in the education field for Cybersecurity, training the next folks to come in and help with this problem, my hat's off to you. We really, really, really need as a country to increase our Cybersecurity capability and our defensive posture when it comes to that. It's not a joke. It's not a fearmongering thing. It's a reality that we're dealing with right now, and I'm really excited to be talking to you guys today on how maybe we can help with some of the challenges that you guys face as educators when it comes to training Cybersecurity personnel.

Does anybody have any questions or anything with that? Or I can just keep going.

Corporate Experience

- 2004 – Won first Prime Cybersecurity Support Contract
- Has held 7 Prime Government Cybersecurity Contracts
- Performance encompasses all levels of CS
- Cybersecurity Personnel encompass ~30% of current billable work
- Recognized by Govini as the #2 Cybersecurity experts across the Department of Defense

[00:06:42]

JUSTIN PARKER: All right, so I think you asked, Steve, our corporate background experience when it comes to this. Sentek has been kind of at the forefront of Cybersecurity, even back when we used to call it ‘information assurance’.

The company has been around for 19 years, and in 2004 we won our very first Prime Cybersecurity Support Contract, and that contract is a contract that we still hold to this day. What that means is the contract is specific to validation, so any system that the United States Navy puts online has to get accredited from a Cybersecurity standpoint, and every single one of those systems goes through that contract that we have. So, we literally see every single Department of Defense Navy system or related system and help make sure its Cybersecurity posture is where it’s at.

In addition to that one, we currently hold over 7 Prime Government Cybersecurity Contracts, we have a couple dozen commercial customers that we support right now, and we also work side by side with some education partners that I can talk about here in a little bit.

Our performance on the services side of the house encompasses all levels of Cybersecurity, so we have folks that do everything from the network security side, folks that are running scans and patches and things like that, all the way up to… We are currently writing the Cybersecurity policy for the Defense Health Agency and everything in between that.

About 30% of our current billable workforce is Cybersecurity, but if you actually include our engineering capability, which makes up about 85% of the company, is either directly or indirectly involved with Cybersecurity because we have moved from build it and then figure out Cybersecurity later to ‘you need to build it with Cybersecurity involved with it. So, every single one of our technical professionals is Cybersecurity trained and worked in Cybersecurity best practices, and I’ll talk a little bit about how we use the Haiku Cyber Range for that.

Just for a tagline, Govini is a Washington D.C.-based assessor of corporate capabilities, and they released a report last year that said Sentek, even though we’re only about 200 people, is actually the #2 Cybersecurity experts in the entire Department of Defense. The only company that ended up ahead of us was Northrop Grumman—that's about, I don't know, $20 billion more than us and several thousands of people!

The big takeaway from this slide is that from a background side of the house we are not a product company per se. We are an engineering and Cybersecurity services company that we came up with the Haiku Cyber Range to actually meet a demand that we were seeing and solve a problem we were having.

So, with that being said, I'll go to the next slide, which is actually the problem.

The Problem

- Traditional interviewing was not garnering favorable results
    - Education/Certification does not equal Technical Capability
- Number of Cybersecurity skillsets continues to expand
- Knowledge required to master a Cybersecurity skillset continues to grow
- Unable to train personnel economically or safely
- Personnel geographically dispersed throughout the world

[00:09:40]

JUSTIN PARKER: So, one thing that we started seeing about 5 years ago was that our traditional interviewing process of scanning a resume, asking some tag high-level questions, was not getting us favorable results.

And please do not take this as a knock to anybody's background, but what we were seeing was we would have people that showed up—example, a woman showed up with a Masters in Cybersecurity, had literally every single certification that we track, but when we got her at the command line of a computer, she actually did not know what to do. The certification and education process was great at testing language and knowledge of high-level book stuff, but when you got into the actual technical capability, we started running into some major challenges.

The next thing was that the Cybersecurity skillset just continues to expand. I use the joke or the example that today you wouldn't just say, "Hey, I need an engineer." Somebody would say, "OK, I need a Mechanical Engineer, I need an Electrical Engineer," something like that as well.

Right now, the mindset is still "I need a Cybersecurity Engineer." What I can tell you is that from a skillset perspective, it is rapidly approaching a level of specialization where the blanket term 'Cybersecurity Engineer' actually really doesn't mean a lot anymore. So, it's changing a mindset from 'this is one person that can do everything' to realistically what you really need is subject matter experts in different facets of Cybersecurity.

What that goes into as well is that the knowledge required to actually master a Cybersecurity skillset also continues to grow. So, what I mean by that is that if you have an expert pen tester, if they were an expert in pen testing a month ago and they didn't learn anything new in that next month, more than likely, they're much less of an expert as well. So, we're seeing an issue where the expansion of skillsets continues to grow, and the depth within each of those skillsets continues to grow at an incredibly rapid pace.

The next thing we ran into, too, is that we're still a relatively small company. We can't afford to build an entire server room with a bunch of different hardware and software that we're loading up into it as well. Then we absolutely don't want some folks learning how to do different types of Cybersecurity or doing penetration testing on the open networks. So, from an economic and safety standpoint, we had a challenge. We couldn't afford to build the physical hardware spaces and buy the software that we needed to do this on the scale that we needed, and we couldn't do it in a way that we wouldn't have, potentially, the FBI kicking down our door if folks were going in and suddenly start trying to use offensive cyber tools to test their pen testing skills or test the defensive skills.

Then the final issue was that we have personnel geographically dispersed literally throughout the entire world. So, if I was able to overcome that economic challenge of creating this standalone network that could do every single thing that I wanted to do that was adaptable, and I could update every single second, I would still have to fly people in or do remote connections or some other way of getting people up to speed and trained on things as well or testing potential candidates on what they were trying to do.

So, we sat in a room and talked about it a while, and we actually looked at a bunch of different offerings out there—none of them really met our needs, so we decided to build our own solution.

The Solution

- Cloud-based Cybersecurity training solution accessible from anywhere with just a browser
- Using gamification, builds practical hands-on skills specific to a Cybersecurity career
- Tailorable and quickly adaptable
- Small development team

[00:13:22]

JUSTIN PARKER: So, what's the solution? So, we decided to go into a cloud-based solution. We currently leverage Amazon Web Services that allows us to create multiple environments, and the technology that we created allows us to spin up and spin down as many different numbers of those environments on demand as we need to.

So, we've moved from a 'hardware footprint buy maintain' lifecycle to a 'develop an environment build' and take that environment and treat it like a utility. So, if we're using it, we're paying for it after we develop it. If we're not using it, we're not paying for it. And that's the technology that we created, leveraging the AWS cloud as our hosting environment within that.

We've also switched over to more of a gamification style of teaching. If you looked at a list of how to do Linux pen testing, you're going to see about 100 to 200 different things that somebody would have to learn how to do. So, how do I take somebody that has zero pen testing and zero knowledgeability and go through a way that's engaging with them and that actually validates their skillset throughout it?

What we decided to do was break these things down into mini micro ranges and scenarios. So, they might start off with a command line that teaches basic Linux commands, like how to open a Directory, how to scan for IPs and things like that. Then, once they've been able to complete that, they check off that range, and then it opens up a couple other ranges as well, like levels in a video game.

So, from that aspect, I'm able to come up with a whole series of connected skillsets that, by the time a person has got to the end of it, they now can not only know how to pen test, but they've demonstrated the capability of how to do that.

I go back to the tailorable and quickly adaptable side of it as well… So, we'll see new mandates or new security information come out for, say, a zero vulnerability. I can create a network—and this gets back to the safety side of the house—and I can actually load that malware into that network and show what happens when that occurs.

So, for our folks that are doing network security defense, we can actually record a video, or they can go in and actually see what happens if the network gets hit with a security vulnerability, so they're more prepared to fight against it. We can also do things like spin up a range, load malware into it with our current security configuration and see if it gets in and then change those security configurations after the fact and then go to the actual operational network and make those changes and know that it's going to protect against that particular vulnerability. That's just an example of tailorable and quickly adaptable.

We have a relatively small development team. Once a range is created and that foundation is built in there, it's like a house. It's a lot easier to add walls and different floors and stuff like that after you've created that initial foundation. So, our development team is actually able to create these environments very, very quickly, and I'll give some examples of that as I go through this, moving to the future.

Then on top of that, once they've created that range, if there's something that a person wants to do, for example, if you're teaching a class and you decide that you're going to use a range as a testing and validation environment one semester, you don't have to go back and create a whole new range for the next semester as your kids pass on all their notes to the students that are following after them, and you have to worry about that as well. You can just go into the existing range and make some changes, load up new versions of software, put in a couple different types of exploits or whatever, and now you have a totally different validation thing that didn't cost hardly any money to go ahead and update at that point in time.

Does anybody have any questions about the solution side of the house? I could literally have spent this entire webinar talking about how Haiku works; I just wanted to kind of hit it at a high note before we get to the demo.

Differentiators

- Cloud-based
- Unlimited ability to scale
- Gamification
- Enterprise solutions

[00:17:44]

JUSTIN PARKER: How are we different? I've kind of talked about this… First off, we're cloud-based. There are a handful of ranges out there that are cloud-based, but we were the first. So, back to differentiators… Cloud-based… There are a couple of ranges that are starting to move towards the cloud-based solution, but we were the first that we were aware of, as far as on a commercial cloud side of the house.

While we do use Amazon Web Services, my cloud developers are actually capable of working in various other different types of clouds to include private clouds. We just use AWS because it’s kind of the industry leader right now when it comes to scalability, which is my next bullet point, and availability. That gets back to that unlimited ability to scale.

So, one of the examples I use when talking about a Cyber Range is from a conference room perspective. I’ve essentially created a conference room for you, and if you want to have one meeting, you can have it in that one. If 1,000 meetings need to take place at the same time, I can replicate that conference room over and over and over again, and you're only paying if you're actually using that conference room at that point in time, so it comes back to an electricity or utility kind of perspective.

For the California Mayors Cup Challenge, which I’ll demo here, which Shawn was involved with heavily, we had 1,300 students accessing the Haiku Cyber Range across the entire state of California in 13 geographical locations for four hours straight, and we didn’t have a single drop.

AWS is the same solution that Netflix uses to host and run their videos, so if there’s one person watching a movie or a million people watching a movie, the technology is able to scale in that way.

I talked about gamification ad nauseum, so I’m not going to bring that up again unless anybody has some questions.

Then the final one is enterprise solutions. So, I talked a little bit about the gamification, and I’ll talk about our offerings as well, but our enterprise solutions group is able to make custom ranges that meet specific customer needs. The California Mayors Cup is an example of it. Some of the Department of Defense things that we’ve done are an example of it, and some of the education offerings we’ve done as well, which essentially allows us to make a tailorable range specifically for a customer base for them to use, like a private range, that meets the requirements of whatever they’re trying to teach, or multiple ranges within that.

How Customers Have Used the Haiku Cyber Range

- Environment Familiarization
- Red Team vs. Blue Team
- Demonstrations
- Governance
- Product Testing
- Skillset Validation

[00:20:19]

JUSTIN PARKER: So, back to get to a previous question: How have customers used the Haiku Cyber Range? We just talked about students that have no experience with Linux whatsoever—so, an environment familiarization side of the house. Since this is a web-based product that doesn't require a plugin or any other kind of software, a teacher could be teaching a class either in person or remotely, pull up their login into the Cyber Range, and display it on a screen and do pointing and clicking. Each individual student could also open up their own range and open up that particular thing and do that clicking and pointing along with the teacher.

We could also embed videos into it as well, so the student is actually working with the actual software. It looks exactly and behaves exactly like the real environment for that period of time that they're using it. So, just general familiarization, as I mentioned, how to do basic Linux commands, how to use technologies like Metasploit, which I'll show a demo of here in a second.

That's a really general powerful way that the range works great in that you don't have to have somebody come into a lab or schedule lab time or whatever. They can access it whenever they need to and point and click to play around with it. If they screw something up, you just restart the range, and they can start from baseline again.

Red Team vs. Blue Team—this was a thing that Shawn had mentioned. For example, a Red Team is an attacker. They're an ethical hacker, and they're trying to do attack kinds of things, like penetration testing and things like that. Blue Team is a defense team, for lack of a better term, so they're going to try to defend the network against hacks.

So, let’s say you have one class that is a Security Engineering course, where they are learning how to do network security, and you have another class that’s an Ethical Hacking class. You can create a range that’s a raw network that you can have your Security Engineering class actually harden it, write policy, upload patches, set configurations to best security practices (NIST framework and things like that), and they can have a set determined time to do that. Then you can take that range and then give it over to the Ethical Hacking class and see if they can penetrate it, and then they can run a pen test and build results from that. So, you can actually get tangible results, and you can use one range to train two different types of skillsets.

Demonstrations—we’ve done ‘The Anatomy of a Hack’ videos before for various industry and education partners to actually show how a hack occurs, how a piece of software works, if you wanted to see something in your network from a product testing standpoint, try something out, and see how it behaves in your network, what it breaks or what it doesn’t break, that’s another thing that it works for as well.

Governance is a big deal. We talk a lot about the sexy parts of Cybersecurity, like penetration testing and Security Engineering and going against bad guys wearing hoods and listening to techno music, but a big, heavy part of Cybersecurity is writing policy, developing processes and procedures, following them and making sure they’re being followed, that you're doing that daily cyber hygiene—every single day.

From a Governance standpoint, we’ve done things like set up a completely blank network, and the students have used that time to actually harden the network and write policy like they’re an IT manager for a company on how that network is supposed to be secured and how the policies and procedures of how it should be acted with.

Then, finally, I mentioned our skillset validation—that was our original need for the Cyber Security Range, and typically, we see these two different ways. One is the competition ones, which are fun, where we do capture-the-flag scenarios, and students go into a range for points—I’ll demonstrate that here in a little bit… Or an actual test type of thing, where, “Hey, you need to set something up," and then the teacher can go afterwards and review their work and see if they actually followed all the processes and procedures that they would have to do for that.

So, those are just some examples. One of our challenges with Haiku is that… A challenge and a good thing is that we haven't found a lot yet that we can't do with it. I'm actually working right now to create a virtual ships bridge for a customer, and we're going to virtualize various different sensors and antennas that can feed data to it, so it can pretend like the ship is anywhere in the world at some point in time, and they can have that type of activity occurring into it.

So, it's kind of like as far as your imagination can take it. We've had a really hard time finding stuff we can't do, for lack of a better term.

Offerings

- Business to Consumer
  - Subscription based
  - Content is developed based on market demand
- Enterprise Solutions
  - Custom environment(s) for business, education, government, and military
  - Content is developed based on customer requirements

[00:25:19]

JUSTIN PARKER: OK, so really quickly, I'll go through the offerings. I kind of touched on this. So, Haiku is actually releasing a business-to-consumer, which is more of a Netflix model. It's a subscription-based model where we have ranges that are available for professionals that want to learn how to do Cybersecurity, students and things like that as well.

The content, though, is set, so it kind of goes back to the Netflix thing—it's based on market demand. I talked about that gamification and that penetration test skillset. That type of path will be in the business-to-consumer model, but it's not tailorable—we're just producing content, producing ranges, and we're building it. We get feedback from the users, and we're releasing things that people want to see.

The Enterprise Solution I talked about as well—it's a custom environment for business, education, government, and military, and we develop it based on customer requirements. That's a much more traditional path of delivering a customized product for you. We can do custom frontends, so it could actually say 'California Community College Cyber Range' up front and just maybe a little tag in the bottom that says 'Powered by Haiku', and then you have the ranges specifically for that course of instruction for there as well.

Customer Feedback

"The Cyber Range is a huge hit with the sailors."

– CAPT Cassol, NAVWAR PMW 750 (after quick 1-week turnaround for proof-of-concept)

"The Haiku range was a great platform for the Mayors Cyber Cup."

– Amy Tong, CIO State of California

"Far better than the previous range that we used, and cheaper."

- LCDR Peyton Price, COMNAVSURFPAC

[00:26:39]

JUSTIN PARKER: So, here are some real quick customer feedback… This is all very, very recent. We had a customer who had a challenge with some of their… A D.O.D. one with their Navy sailors not knowing how to do a patch and scan range, so that was based out of an inspection that they basically failed.

So, over the weekend, we created an environment. We loaded up the same software that they learned how to scan in, and we gave it to the customer the next week. They were able to train all those IT sailors how to actually do the scanning from their workstations in Washington and Tokyo, Japan, and all those places around the world, and it was turned around, like I said, in less than a week.

The California State CIO attended the California Mayors Cup Challenge, and she saw how well the platform worked for that because she's seen a couple of them over different times.

Then Lieutenant Commander Peyton Price has actually had us do a couple of different hackathons for the United States Navy. We did one here in San Diego, and we did one in Korea—in South Korea, not North Korea—where we actually did that at a Korean Navy base using Korean Navy hardware (their laptops), and it was the first ever competition between the United States and South Korea from a Cybersecurity competition. We flew out there to just kind of be there to help, but we brought no hardware with us or anything as well, and that went really, really well.

The Partners

- Amazon Web Services
- AttackIQ
- ESET
- NAVWAR PMW 750
- COMNAVSURFPAC
- COMNAVFORKOR
- San Diego Cyber Center of Excellence
- University of San Diego
- California Cyber Hub
- California Mayors Cup

[00:28:14]

JUSTIN PARKER: Here are some of our partners… We use AWS, AttackIQ, ESET… ESET has actually asked us to test some of their products before they release them to market, so we've loaded up some of their software and firewalls and stuff like that into Haiku ranges and then ran attack scripts against to validate, and they've used that as validation that, 'hey, our product stops 99% of known vulnerabilities' and things like that as well.

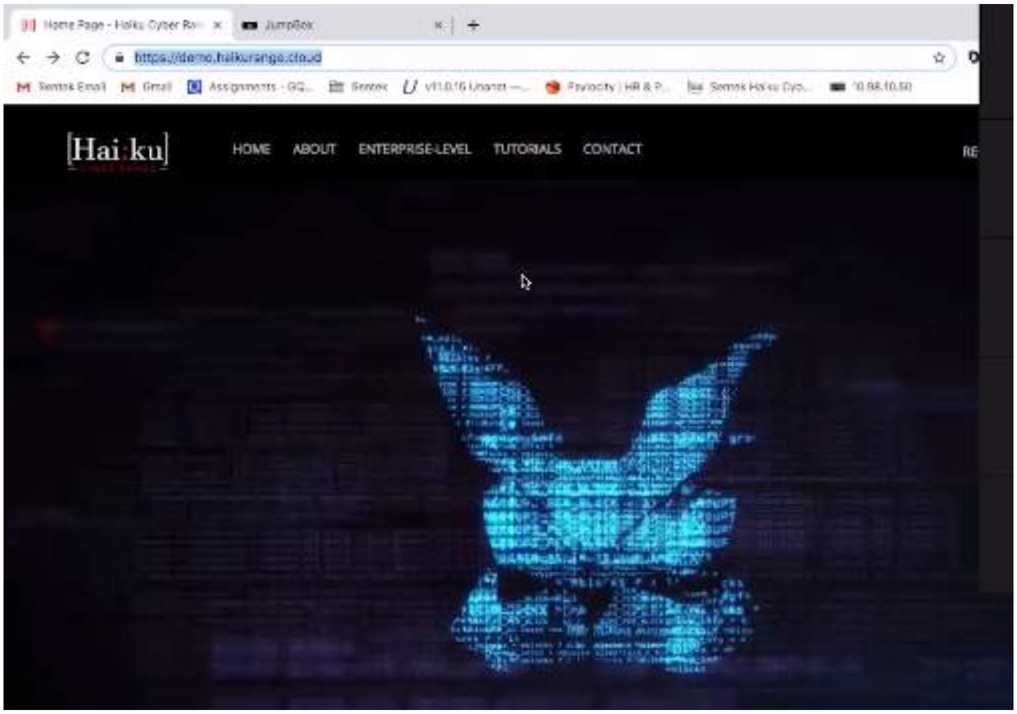
Various military partners… Eric sits on the board of the San Diego Cyber Center of Excellence, and we currently are partnered with the University of San Diego, and we're building a range for them right now for their Master of Cybersecurity course as well.

So, with that being said, before I start my demo, were there any other questions or anything like that of what I presented? That was a lot of material I know that I covered in a relatively short period of time.

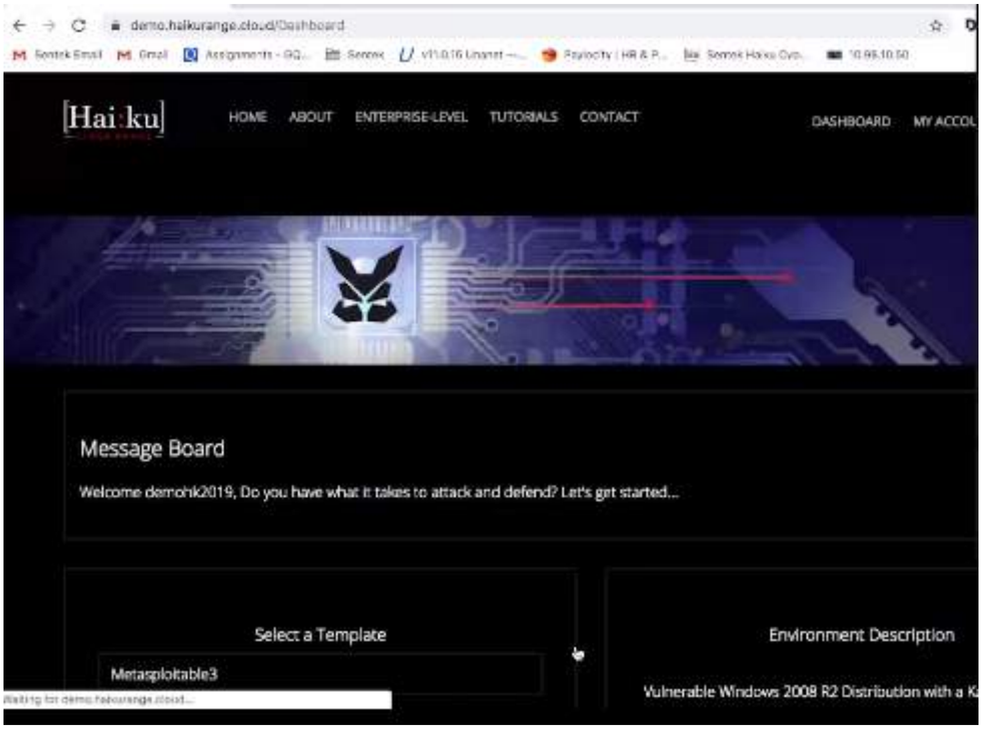
OK! All right!

[00:29:18]

Haiku Cyber Range Demo



JUSTIN PARKER: So, let's get into the demo side of the house. OK, can everybody see the Haiku landing page? So, once again, this is just through our URL. I haven't loaded any type of software in there or anything like that. I'm going to press 'Login'—you get to a general login screen with Username and Password, very simple.



Message Board

Welcome demohk2019, Do you have what it takes to attack and defend? Let's get started...

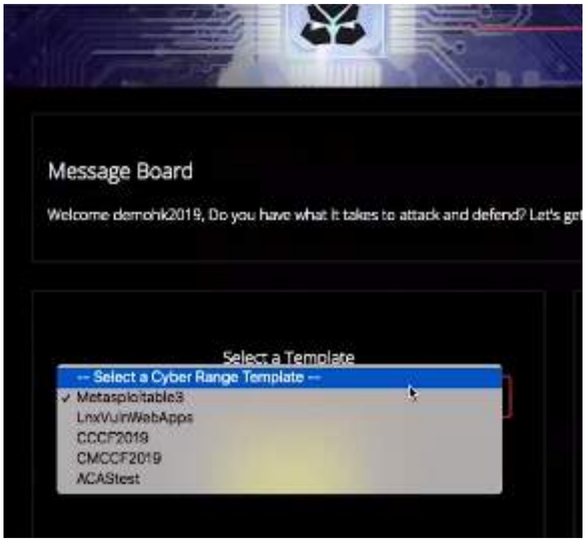
Select a Template

Metasploitable3

Environment Description

Vulnerable Windows 2008 R2 Distribution with a K

You log into the range, and you get… This is our demo account, so we don't have a ton of stuff in here, but we have a basic Message Board. And as you can see, we have different Tutorials that we can click on, if people want to learn how to use certain different types of tools. If they have an issue of contacting we have a Dashboard that allows people to track what they've done and what they haven't done, if you need to make any updates to your account, things like that as well.



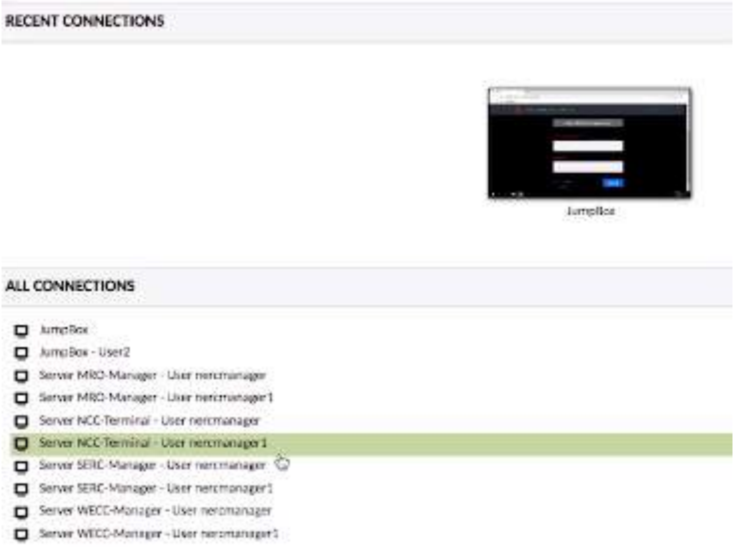
Message Board

Welcome demohk2019, Do you have what it takes to attack and defend? Let's get

Select a Template

-- Select a Cyber Range Template --
✓ Metasploitable3
LnxVulnWebApps
CCCF2019
CMCCF2019
ACAStest

Right here, we have our Template select. I've only loaded up a couple different ranges in here, but if I click on a range, it will give an environment description. I'm going to do the California Mayors Cup one first, and we'll see how we're doing on time after that. I like to do this range because it's definitely one of our more advanced ranges, and it really demonstrates some of the power of the tool and some of the different ideas that you can do with it.



RECENT CONNECTIONS

JumpBox

ALL CONNECTIONS

- JumpBox
- JumpBox - User2
- Server MRO-Manager - User nercmanager
- Server MRO-Manager - User nercmanager1
- Server NCC-Terminal - User nercmanager
- Server NCC-Terminal - User nercmanager1
- Server SERC-Manager - User nercmanager
- Server SERC-Manager - User nercmanager1
- Server WECC-Manager - User nercmanager
- Server WECC-Manager - User nercmanager1

So, real quick, I'll go ahead and open it up. As you can see, it just pops up immediately in a different window. I think the only thing that we've had people do sometimes is they have to disable their popup blocker, but that's pretty much it.

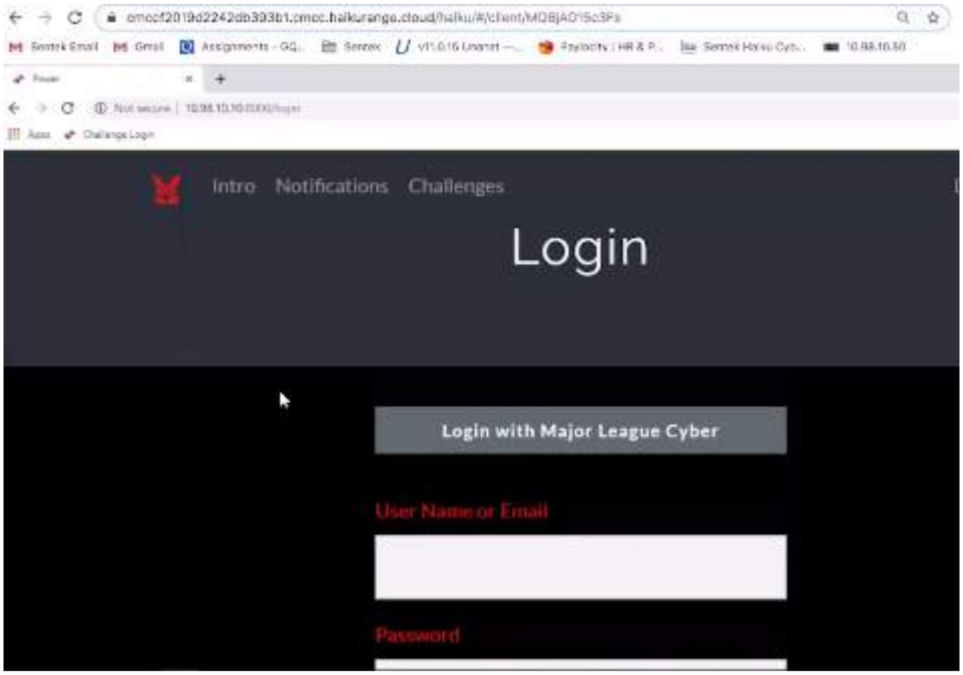
Now, within the range here, you see that we have a variety of different types of boxes. What we did for the California Mayors Cup Challenge is we actually created an entire virtualized United States power grid. We had demonstrated that by having these servers for these different power grid regions.

JumpBox

[00:31:25]

JUSTIN PARKER: Another thing that we have here as well that's very unique to us is what's called the 'JumpBox'. So, I mentioned earlier that security is a great aspect within the Haiku Cyber Range, is that you've created a self-contained virtual environment that you can do anything you want to in, to include loading up viruses and other bad stuff. We can do penetration testing and things like that, but in the real world, I don't care how good your Cybersecurity people say they are—they Google!

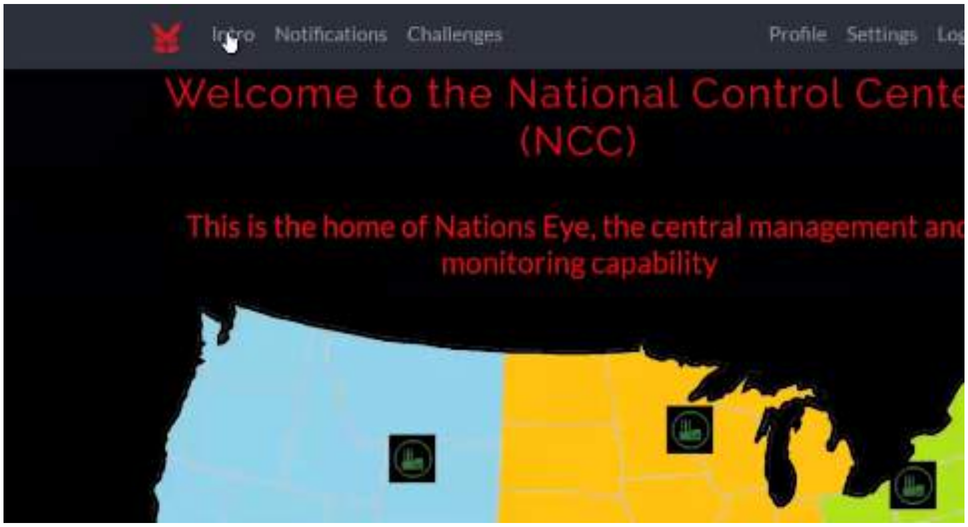
So, a JumpBox actually allows us… It's one of our technologies to jump outside of the range and access the real internet and things like that, without compromising the security of the box that you're in.



We use the JumpBox in the California Mayors Cup to actually access the scoring server. This one was a competition that was for middle school and high school students, and it was particularly challenging because we had every single type of skillset that you could have from, like

I said, kids that literally just knew how to Google all the way up to what I would call Cybersecurity savants.

We had a challenge when we did that because we had to come up with an engaging four-hour competition that would be good for all those different levels of skillsets. We used a scoring server to create all different types of challenges and things like that as well.

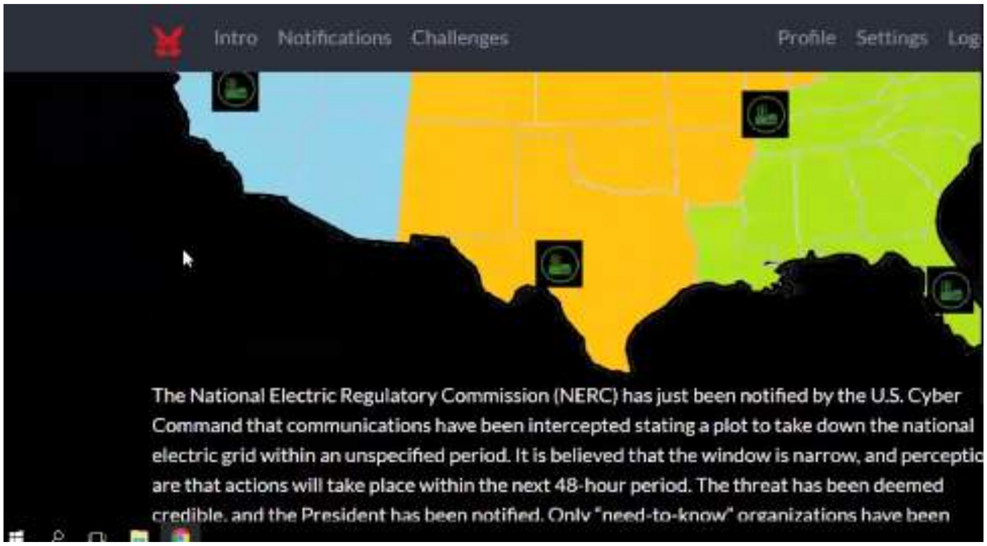


Welcome to the National Control Cente

(NCC)

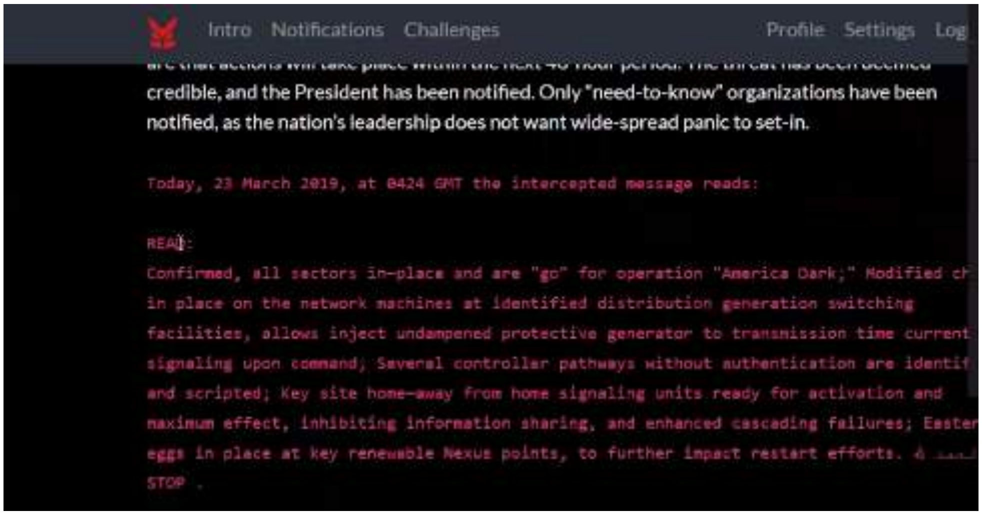
This is the home of Nations Eye, the central management anc monitoring capability

So, the intro… One of the things, too, they wanted us to do was a lot of governance. So, we gave a background, we gave a bunch of different documentation and paperwork, we essentially gave them a network policy for this imaginary power grid that we built.



The National Electric Regulatory Commission (NERC) has just been notified by the U.S. Cyber Command that communications have been intercepted stating a plot to take down the national electric grid within an unspecified period. It is believed that the window is narrow, and perceptic are that actions will take place within the next 48-hour period. The threat has been deemed credible, and the President has been notified. Only "need-to-know" organizations have been

Within that, they have the introduction thing, which gives some overview that, essentially, they are a Cybersecurity response team and that over the next 48 hours there is a threat that's been deemed credible that's going to be attacking the nation's power grid.

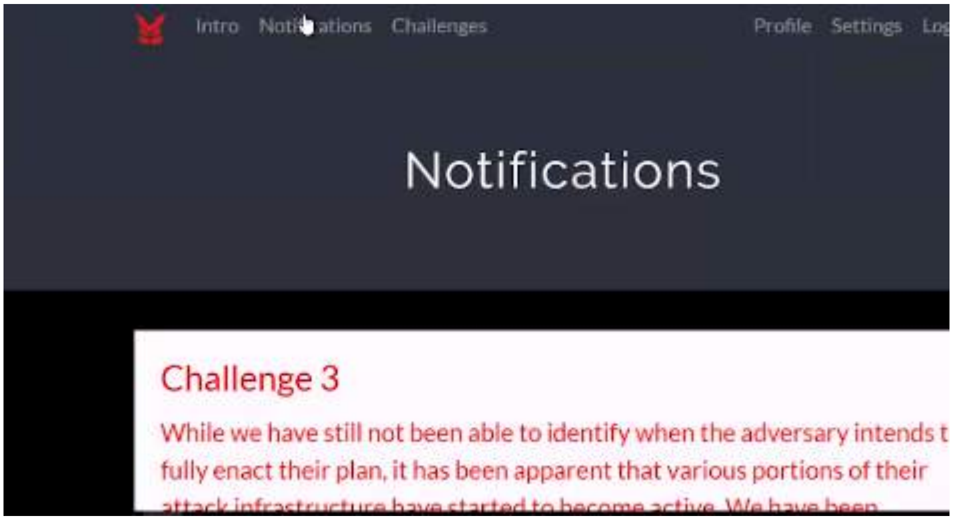


are that actions will take place within the next 48 hour period. The threat has been deemed credible, and the President has been notified. Only "need-to-know" organizations have been notified, as the nation's leadership does not want wide-spread panic to set-in.

```
Today, 23 March 2019, at 0424 GMT the intercepted message reads:

READ:
Confirmed, all sectors in-place and are "go" for operation "America Dark;" Modified ch
in place on the network machines at identified distribution generation switching
facilities, allows inject undampened protective generator to transmission time current
signaling upon command; Several controller pathways without authentication are identif
and scripted; Key site home-away from home signaling units ready for activation and
maximum effect, inhibiting information sharing, and enhanced cascading failures; Easter
eggs in place at key renewable Nexus points, to further impact restart efforts.
STOP .
```

And they have some information that's come as well, and throughout the challenge, they would get notifications that would pop up. So, that was another way that we kept it engaging over 4 hours. We didn't just release all the information at once. It was like the real-world scenario where new information is presented throughout the course of the event.



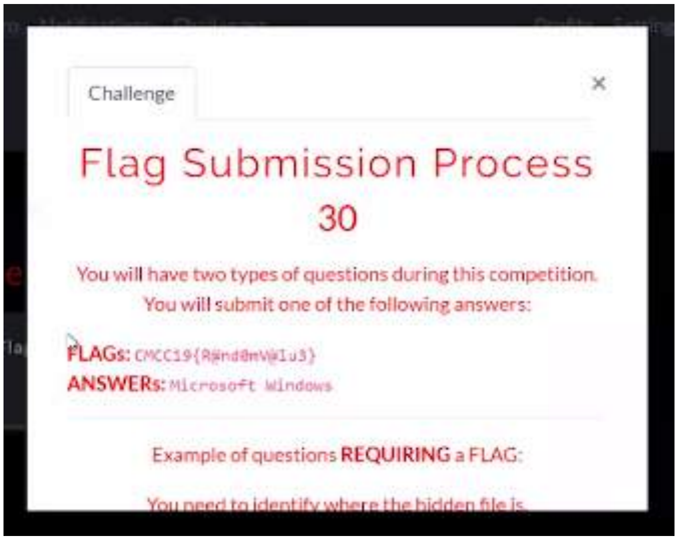
Notifications

Challenge 3

While we have still not been able to identify when the adversary intends t fully enact their plan, it has been apparent that various portions of their attack infrastructure have started to become active. We have been

So, they would get these notifications that would pop up, and as they popped up, new things and new information that they would need to be able to do different challenges occurred. For the purposes of the demonstration, I've already unlocked all of the different challenges, but over the course of this event, about every 45 minutes, they would get another challenge that prompted them with new information, and it unlocked new different types of challenges for them to do.

So, if I go to the Challenges tab here… Once again, we were trying to do it in a way that would drive them to learn how to use the range while they were using it but at the same time keep it in a game way.



Flag Submission Process

30

You will have two types of questions during this competition.
You will submit one of the following answers:

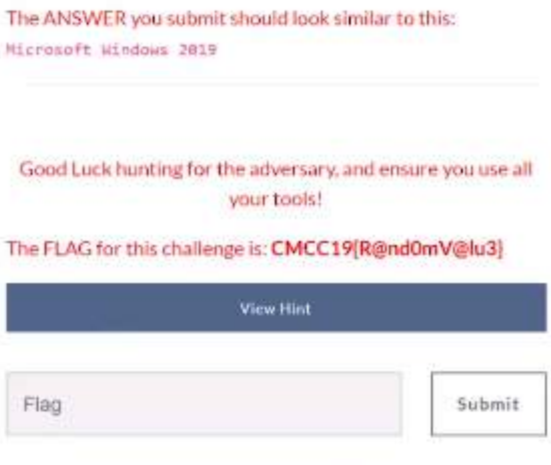
FLAGs: `CMCC19{R@nd0mV@lu3}`
ANSWERs: `Microsoft Windows`

Example of questions **REQUIRING** a FLAG:

You need to identify where the hidden file is.

This is just teaching them how to submit a flag. It basically says we have two different types of questions. For this competition, the customer wanted us to teach basic cybersecurity knowledge and also test the ability to do forensics and other different types of cybersecurity activities within that.

So, we have two different types of Flags and Answers. The Flag is something they would actually physically go into the range and find (I'll demonstrate that here in a little bit). Answers that were text-based were based on their knowledge or their ability to go find knowledge as well.



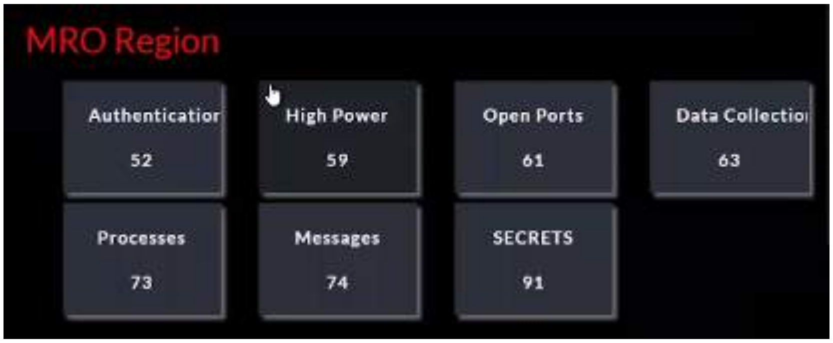
The ANSWER you submit should look similar to this:

`Microsoft Windows 2019`

Good Luck hunting for the adversary, and ensure you use all your tools!

The FLAG for this challenge is: **CMCC19{R@nd0mV@lu3}**

So, it just goes through an example of that, like "What is the current version of Window server?" that they're using, and then they have to actually enter a Flag to unlock the thing. We also have hints as well to make it a little bit more, and we made it so that the hints cost points, but for this one, it's free. For most of the challenges, people had hints that they could unlock, and that was something they had to work on as a team, whether or not they wanted to burn some of their points to try to solve something.



MRO Region

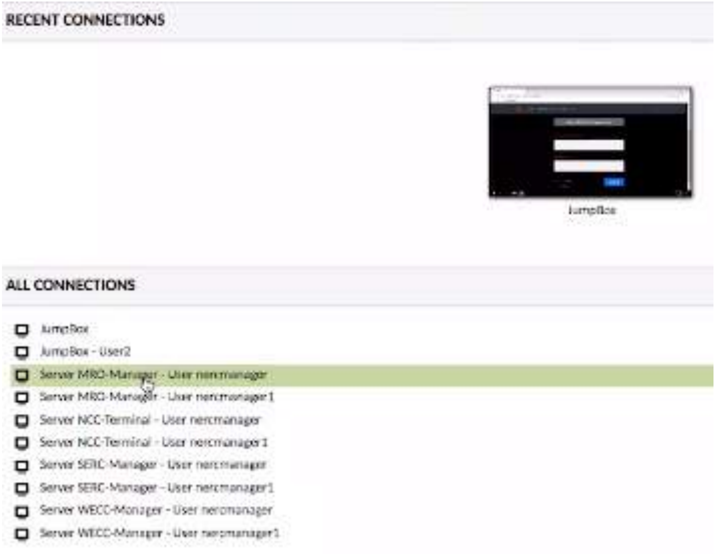
Authenticatior 52	High Power 59	Open Ports 61	Data Collectioi 63
Processes 73	Messages 74	SECRETS 91	

I'm going to go ahead and enter the Flag here and hit Submit, and I got a 'Correct.' Once I've done that, you can see that now all of the different challenges have been unlocked. There are ones based on each region:

- MRO Region
- SERC Region
- NCC Region

- WECC Region

And then they have Game, and then they have National Electric Grid as well.



RECENT CONNECTIONS

JumpBox

ALL CONNECTIONS

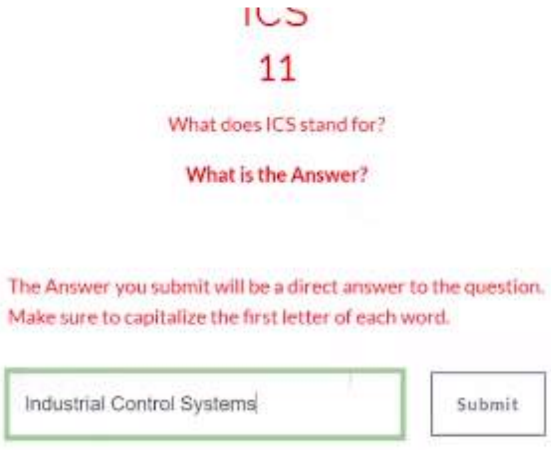
JumpBox
JumpBox - User2
Server MRO-Manager - User nercmanager
Server MRO-Manager - User nercmanager1
Server NCC-Terminal - User nercmanager
Server NCC-Terminal - User nercmanager1
Server SERC-Manager - User nercmanager
Server SERC-Manager - User nercmanager1
Server WECC-Manager - User nercmanager
Server WECC-Manager - User nercmanager1

So, if I go back to the actual range here, you can see that those different servers for all those different regions that we talked about, and if they go to the Intro slide and get that visualization, they can see where all these different places are around from a country perspective.

Basic Challenges

[00:36:20]

JUSTIN PARKER: So, back in the Challenges… I mentioned that we did some basic ones to test cybersecurity knowledge. ICS is, basically, pretty simple. What does ICS stand for? This is aimed at the students that don't have a lot of cybersecurity knowledge, and they can kind of learn stuff while they're actually playing the game. We can tailor the questions so, if they answer in all caps or if they don't put anything in there as well…



ICS

11

What does ICS stand for?

What is the Answer?

The Answer you submit will be a direct answer to the question.
Make sure to capitalize the first letter of each word.

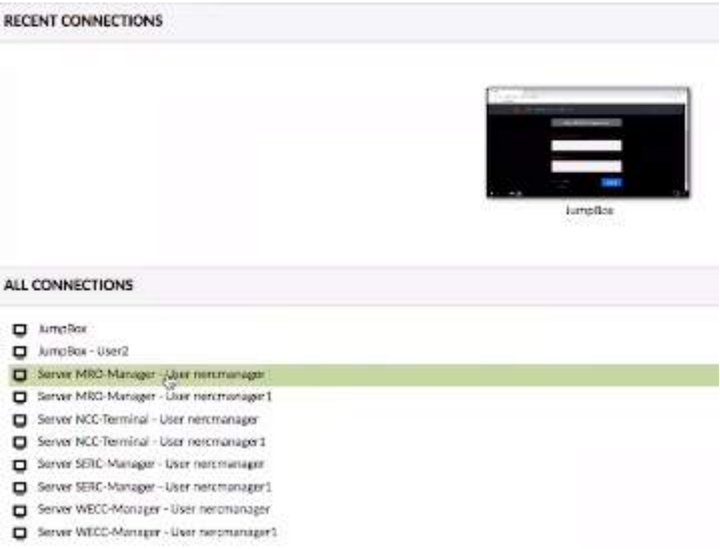
Industrial Control Systems

Just out of curiosity, does anybody on the phone know what ICS stands for in Cybersecurity? All right, I'm getting a 'no' across the board. So, Industrial Control Systems is the answer to that. Submit—and correct. So, I got 11 points for that.

Another thing that we did here that I'm not demoing today is we actually have a live scoreboard that was actually broken out by competition region. So, while the competition was going on, the proctors of the competition were able to display on the big screen the active scoring as it was going on throughout the competition, so you would see where your team was falling and things like that as well.

We could do that obviously for an instructor perspective, where you can have a scoring engine or something else you can log into and see your students' progress as they go through some kind of evaluation.

Another good one to do that actually forces them into going into the range to learn something is the familiarization one. So, within there, we have a Familiarization that says, "What is the name of the system monitoring the electric grid?" This actually drives them into the range to actually learn how things are in there and learn how it's set up.

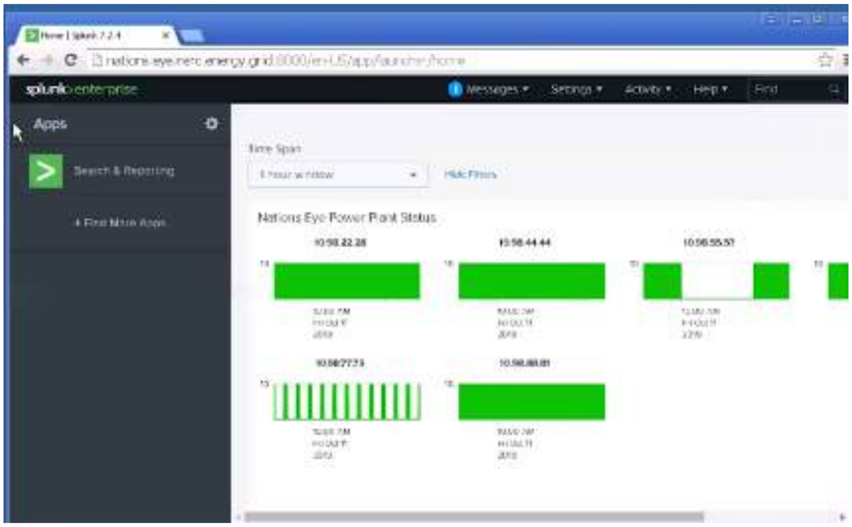


RECENT CONNECTIONS

JumpBox

ALL CONNECTIONS

- JumpBox
- JumpBox - User2
- Server MRO-Manager - User nercmanager
- Server MRO-Manager - User nercmanager1
- Server NCC-Terminal - User nercmanager
- Server NCC-Terminal - User nercmanager1
- Server SERC-Manager - User nercmanager
- Server SERC-Manager - User nercmanager1
- Server WECC-Manager - User nercmanager
- Server WECC-Manager - User nercmanager1

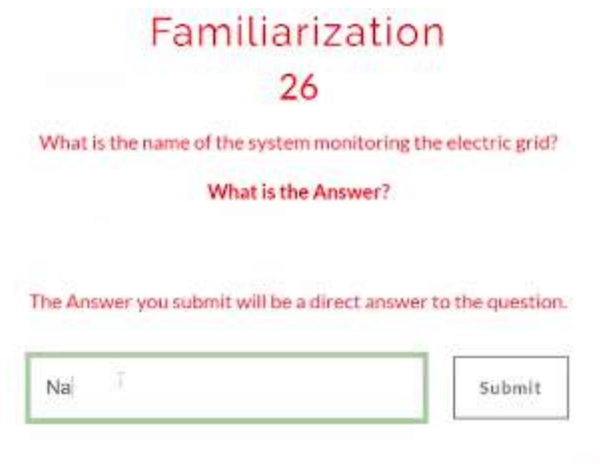


So, if I access the MRO Manager, they'll see that we've added a Splunk tool in here, a piece of software, and we've run scripts in the background to make Splunk behave in a certain way. Now, each one of these IP addresses actually represents one of the different power stations throughout the entire nation.

As you can see here, there are different behaviors showing at once. There's one showing up and showing down. Splunk is a tool that is very common that allows you to visualize your network activity. It familiarizes students with something they would most likely see.

Another fun thing that we did for this challenge as well is we actually loaded up older versions of operating systems in here. So, this is a Windows server 2003. That is the type of stuff they would see if they went to a power station or some kind of municipal network. They're not going to see the latest and sexiest stuff, so it also teaches them to learn how to use different versions of operating systems and how they work as well.

This works exactly like it works for the real world. They can change the different time windows and get different types of displays as it goes on in real life, but that being said, the thing that monitors the grid is the Nations Eye.



Familiarization

26

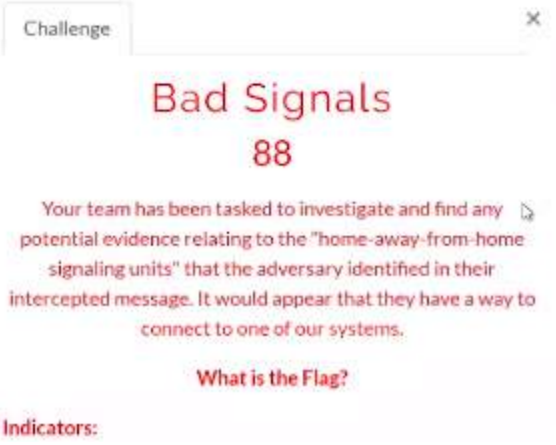
What is the name of the system monitoring the electric grid?

What is the Answer?

The Answer you submit will be a direct answer to the question.

Na

So, I'm going to go back here to my question and answer, and I'm going to go ahead and enter 'Nations Eye' and hit 'Submit', and I got it correct, so I've got 26 points off of that. That was just to show them how to go in there. So, now we can do some harder things that actually are going to test cybersecurity, different types of skills.



Challenge

×

Bad Signals

88

Your team has been tasked to investigate and find any potential evidence relating to the "home-away-from-home signaling units" that the adversary identified in their intercepted message. It would appear that they have a way to connect to one of our systems.

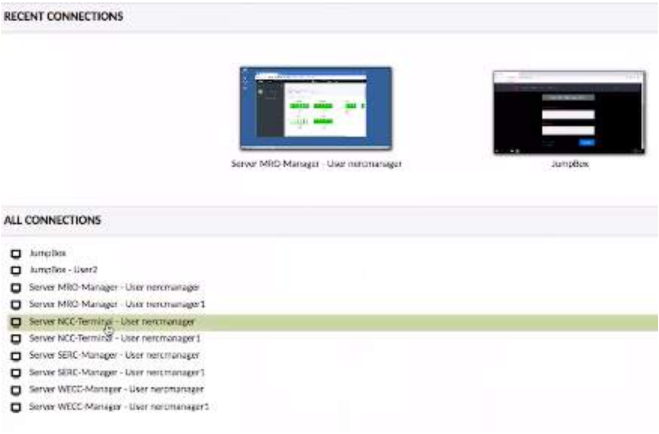
What is the Flag?

Indicators:

So, if I go into the NCC Region, there's one called 'Bad Signals'—now, this one is worth 88 points, so this is a pretty challenging thing.

"Your team has been tasked to investigate and find any potential evidence relating to the 'home-away-from-home signaling units' that people are using to intercept messages." You've got some intel that somebody is intercepting messages between power stations, and your job is to go find out where that's at.

You get some indicators that the Threat Actor is known to configure backdoors into systems, and this is letting them know that they're going to be looking for a Flag like that. They can also unlock a hint as well. So, for this one, it gives you an opportunity to say, "Are you sure you want to do this—it's going to cost you some points?" I'm going to go ahead and click 'Yes', and it says, "Examine the open ports and services."



RECENT CONNECTIONS

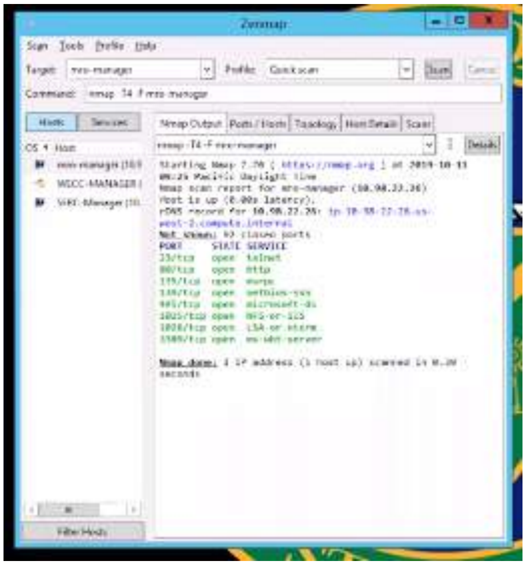
Server MRO-Manager - User nercmanager

JumpBox

ALL CONNECTIONS

- JumpBox
- JumpBox - User2
- Server MRO-Manager - User nercmanager
- Server MRO-Manager - User nercmanager1
- Server NCC-Terminal - User nercmanager
- Server NCC-Terminal - User nercmanager1
- Server SERC-Manager - User nercmanager
- Server SERC-Manager - User nercmanager1
- Server WECC-Manager - User nercmanager
- Server WECC-Manager - User nercmanager1

So, I'm going to go into, since I know this is in the NCC Region… I'm going back out of here, and I'm going to go into the NCC-Terminal.

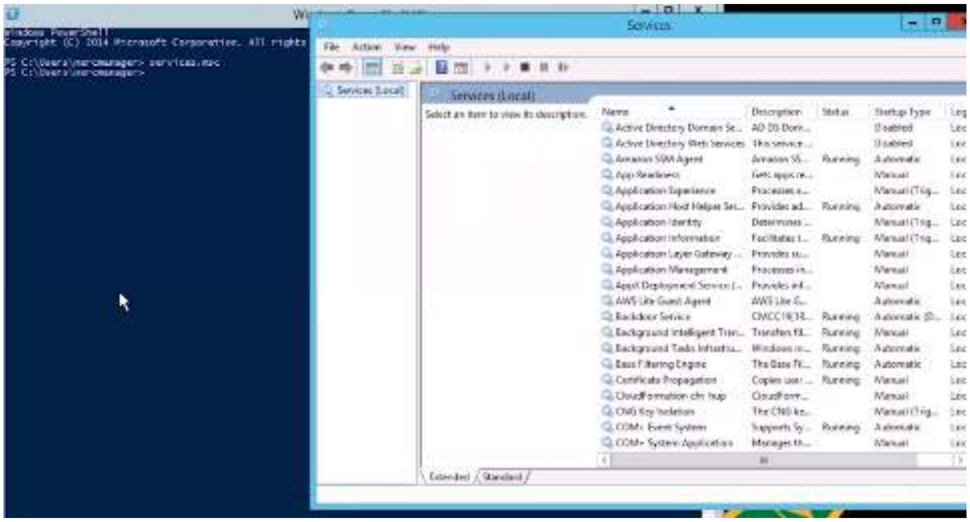


Target: nrc-manager
Profile: Quick scan
Command: nmap -T4 -F nrc-manager

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-11
09:25 Pacific Daylight Time
Nmap scan report for nrc-manager (10.98.22.26)
Host is up (0.00s latency).
rDNS record for 10.98.22.26: ip-10-98-22-26.us-
west-2.compute.internal
Not shown: 92 closed ports
PORT     STATE SERVICE
23/tcp   open  telnet
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.30
seconds
```

So, within the NCC-Terminal, I'm going to go ahead and open a command line, and I'm going to run a services command within the command line to get everything opened up here…



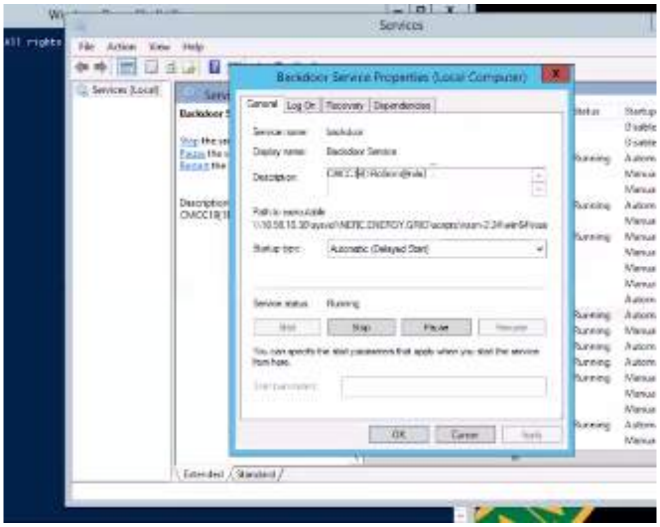
```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights
PS C:\Users\nrcmanager> services.msc
PS C:\Users\nrcmanager>
```

Services (Local)

Select an item to view its description.

Name	Description	Status	Startup Type	Log
Active Directory Domain Se...	AD DS Dom...		Disabled	Loc
Active Directory Web Services	This service ...		Disabled	Loc
Amazon SSM Agent	Amazon SS...	Running	Automatic	Loc
App Readiness	Gets apps re...		Manual	Loc
Application Experience	Processes a...		Manual (Trig...	Loc
Application Host Helper Se...	Provides ad...	Running	Automatic	Loc
Application Identity	Determines ...		Manual (Trig...	Loc
Application Information	Facilitates t...	Running	Manual (Trig...	Loc
Application Layer Gateway ...	Provides su...		Manual	Loc
Application Management	Processes in...		Manual	Loc
AppX Deployment Service (...	Provides inf...		Manual	Loc
AWS Lite Guest Agent	AWS Lite G...		Automatic	Loc
Backdoor Service	CMCC19{1B...	Running	Automatic (D...	Loc
Background Intelligent Tran...	Transfers fil...	Running	Manual	Loc
Background Tasks Infrastru...	Windows in...	Running	Automatic	Loc
Base Filtering Engine	The Base Fi...	Running	Automatic	Loc
Certificate Propagation	Copies user ...	Running	Manual	Loc
CloudFormation cfn-hup	CloudForm...		Manual	Loc
CNG Key Isolation	The CNG ke...		Manual (Trig...	Loc
COM+ Event System	Supports Sy...	Running	Automatic	Loc
COM+ System Application	Manages th...		Manual	Loc

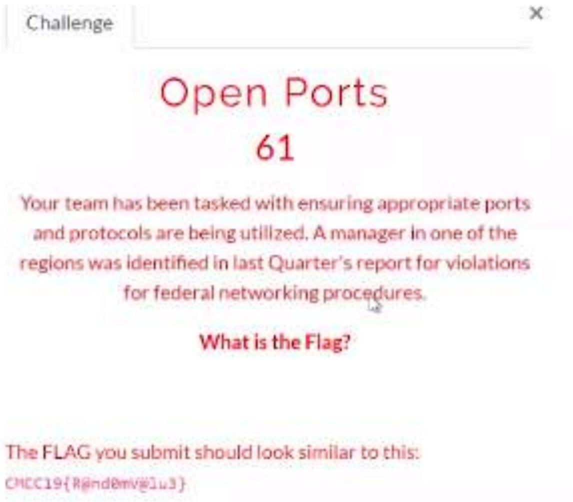
So, this is showing all the services that are running within this server right now. As I scroll through here, I found something that looks kind of interesting that says 'Backdoor Service'. If I double-click on that and I look at the description, there's my Flag…



Service name: backdoor
Display name: Backdoor Service
Description: CMCC19{[illegible]}
Path to executable:
\\10.58.15.30\sysvol\NERC.ENERGY.GRID\scripts\[illegible]
Startup type: Automatic (Delayed Start)
Service status: Running
You can specify the start parameters that apply when you start the service from here.
Start parameters:

So, I've identified what service is allowing for this intercepted message, and now I have the Flag that I can go in here and enter into the Bad Signals and get those points. I'll do one other little, quick technical one, just so you guys can see how we're using this from this game perspective. A good one to do is 'Open Ports'.

Open Ports



Open Ports

61

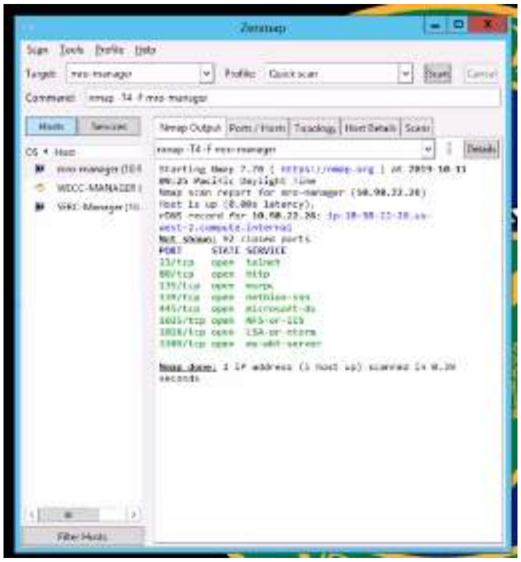
Your team has been tasked with ensuring appropriate ports and protocols are being utilized. A manager in one of the regions was identified in last Quarter's report for violations for federal networking procedures.

What is the Flag?

The FLAG you submit should look similar to this:
CMCC19{R@nd0mV@lu3}

[00:42:02]

JUSTIN PARKER: So, this is making sure that all ports and protocols are being properly utilized and servers like this…



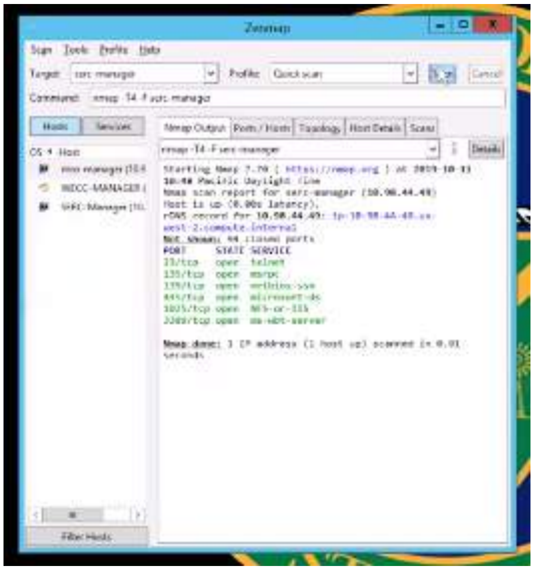
Target: mro-manager
Profile: Quick scan
Command: nmap -T4 -F mro-manager

```
nmap -T4 -F mro-manager
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-11
09:25 Pacific Daylight Time
Nmap scan report for mro-manager (10.90.22.28)
Host is up (0.00s latency).
rDNS record for 10.90.22.28: ip-10-90-22-28.us-
west-2.compute.internal
Not shown: 92 closed ports
PORT     STATE SERVICE
23/tcp   open  telnet
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.39
seconds
```

I'm not going to unlock a hint this time because, through my range Familiarization, I saw that I have, within this terminal right here, a Zenmap server. Zenmap is a scanning tool that's very common that most of your students will probably have some familiarization with, or should have familiarization with, and based on the governance, I know the different target names for all of the servers on my network.

So, what I'm going to do is I'm going to run a scan on each server and see if there are any ports that show up that look silly…



Target: serc-manager
Profile: Quick scan
Command: nmap -T4 -F serc-manager

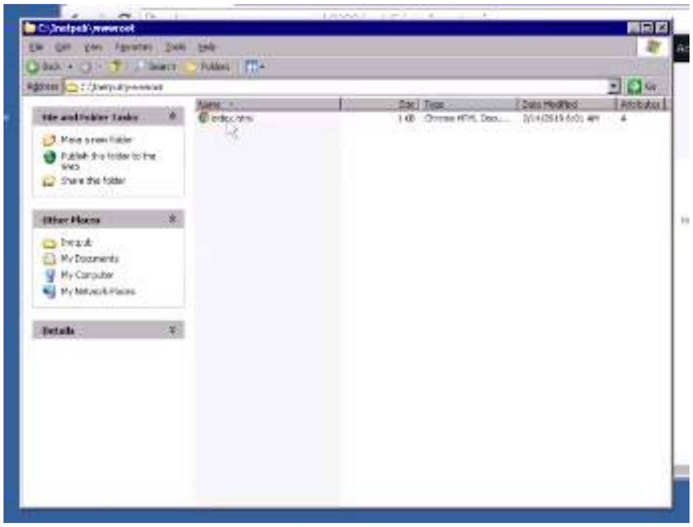
```
nmap -T4 -F serc-manager
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-11
10:48 Pacific Daylight Time
Nmap scan report for serc-manager (10.90.44.49)
Host is up (0.00s latency).
rDNS record for 10.90.44.49: ip-10-90-44-49.us-
west-2.compute.internal
Not shown: 94 closed ports
PORT     STATE SERVICE
23/tcp   open  telnet
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.91
seconds
```

So, SERC (and this goes back to understanding proper ports and protocols)… This is, like I said, a very advanced kind of question for those cybersecurity savants. Believe it or not, many, many students got this question right, or many different teams got it right.

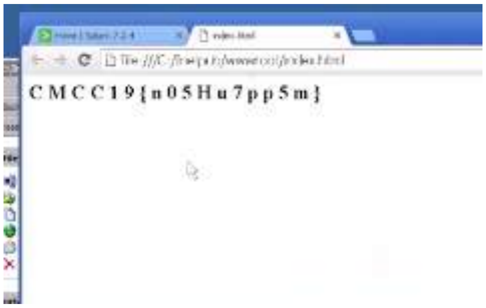
So, I run SERC. There's nothing there that's really pointing out to me that could look weird. I'll run one on the WECC one, do a quick scan on that, and there's nothing there, same ones as well.

If I go to the MRO one, though, and run a quick scan, there's one showing here that's 80—port 80 is open, and that doesn't make any sense. So, let me go back here to the MRO Manager, and I'm going to click on that. Within the MRO Manager, I'm going to take a look at my root file. So, let's open up My Computer, and I'm going to access the root file and see if there's anything in there.



Name	Size	Type	Date Modified	Attributes
index.htm	1 KB	Chrome HTML Docu...	[illegible]	A

OK, there's this index file in there—it opens up in Chrome.



CMCC19{n05Hu7pp5m}

There’s my Flag. So, I’ve identified where that port is working at and where that’s happening from that perspective. I’ve got my Flag, and I go in and do it.

Another aspect behind this, too, is this requires teamwork. So, if a team wants to… There were anywhere between 3 to 8 students working on a team, and they were all in their particular range at that point in time. So, it also worked teamwork in there as well.

What I saw the good teams do was say, “Hey, Bob, you go in there and scan this network and look for anything weird. You scan that one. You scan that one. You scan that one.” Then they were able to go and work as team to go find things as well.

I obviously jumped to the quick one because I know where the answers are, but ideally, this kind of question should take even a talented team anywhere from 20 minutes to half an hour to try to work through and figure out.

[00:44:40]

Questions

JUSTIN PARKER: So, that’s, really quick here, a demonstration of the CMCC Range. Now, we use this as a capture-the-flag scenario, but there’s nothing that kept us from doing this as one of those other type of scenarios I talked about, a Red Team vs. Blue Team where they can harden the network, and somebody can try to penetrate it, a policy one where they literally get a raw network and throughout the course of the semester actually write Cybersecurity policy for that network and best practices. They can patch the old software. They can upload new software into it. All kinds of stuff like that as well is capable within this range.

Just so you guys know, from a dollar standpoint, depending on how many students you have, you're looking at anywhere between $10 to about $35 a day to run a range for a 24-hour period. AWS is neat in that it charges by the hour. So, if your students are accessing this during the course of a one-hour class, you're only paying for the time period that they’re accessing it during that particular course. So, just so you know from there.

Are there any other questions about this one? I’ll show a couple other little ranges real fast, just for the familiarization side of the house.

Sorry, I’ll wait for questions, if anybody has any. All right, and we’re kind of getting tight on time here, so I’ll just show this really fast.

[00:46:07]

STEVE WRIGHT: Yeah, and Justin, I do have a question—this is Steve Wright. The next question anyone is going to have is ***how much? I’m glad you shared the cost per student—is that total cost going in, and everything is accessible from any connected laptop or computer? I mean how does this work in a student environment?***

[00:46:07]

JUSTIN PARKER: Yeah, from a cost perspective, what we do, typically, is we sit down (and this is from an Enterprise Solutions perspective), and we get with the customer, essentially, at the end of the day, and we say, “OK, what are you trying to do here?”

It basically comes down to how long it’s going to take us to develop it—there’s a development cost associated with it. The CMCC Range took us about three weeks to develop, and that development cost was about $10,000 per week to develop it. Once it’s developed, then you're only paying for the utility side of the house, and the CMCC Range at this scale right now costs about $30 a day.

Now, one of the other neat things about AWS is you can essentially buy futures in it. So, if you agree with AWS that you're going to be using this over the course of a year, and you can pre-purchase a block of time. It can cut your operating cost down anywhere from 20% up to 70%, depending on what type of appliances you're using. That’s why I said, “Hey, this could actually cost about $10 a day to run,” from that perspective, per student.

I’ve also had teachers come and try to back us into it, like, “Hey, this is what we want to do, but we want the cost per student to be at or less than a textbook for a semester.” So, if you can keep what their cost would be, about $200… And you can text these various different types of requirements and skillsets, then we can come up with a solution or attempt to come up with a solution that meets those needs.

So, from a cost perspective, it really depends on the complexity of the range, how many different servers that you guys are using, and how many different cores are within those servers that you need to do. I like to do the micro-range offering if you're trying to test a variety of skillsets because, for this particular competition, we had all these different servers running and all these different services in the background for this 4-hour event.

But let’s say you wanted to teach that one thing I just showed with being able to scan open ports and protocols. You really only need one server with one or two cores to do that, and that cost can be $5 a day. Then, once you've demonstrated that they can do the Zenmap thing and they know how to do it, then you do another little micro-range along the way, too. Then, maybe at the end, you have some kind of competition or overall skillset where you have a bigger range that's more expensive, but you're only using it for that period of time during testing.

I apologize—I'm not trying to give a roundabout answer, but for the Enterprise Solutions, it really kind of depends. For the business-to-consumer side of the house, we're targeting a price range of about $35 per month, but once again, that content is going to be developed… You don't have control over what kind of content comes out of that—does that make any sense?

[00:49:28]

STEVE WRIGHT: Oh, yeah! It's good to know the options. Those sound workable. I mean, obviously, if we were able to corral our interest statewide and look at a customized setting, that would be advantageous to do. Otherwise, your business-to-consumer might be advantageous because a lot of colleges just like to do it their own way, and that's always our challenge. Even though we're a big organization of 112 or more colleges they tell me, we all think differently, and we do not necessarily operate as a single buying entity at all, so it's good to know the options. That's very good. Thanks.

If anybody has any questions, if you want to speak up now or write them in chat, we're reading.

[00:50:12]

SHAWN MONSEN: Hey, Justin, it's Shawn.

[00:50:13]

JUSTIN PARKER: Hi, Shawn!

[00:50:16]

SHAWN MONSEN: Thanks for that. It was really interesting. ***I'm just thinking about how we might be able to use this in a classroom, and how easy is it?*** Let's say we were looking at a scenario where, generally speaking, at the community colleges, we have a lot of colleges now that are offering the Security+ class, which is the basic intro Security class. Then, again, a lot of colleges that are offering the Ethical Hacking class, which either leads to a CEH certification or a Pen Test+ certification.

So, the question is, how easy is it or how easy would it be to try to create some labs around those types of curriculum, the Security+ and the CEH or Pen Test+ certifications, for use in the classroom?

[00:51:17]

JUSTIN PARKER: So, Shawn, I'm glad you asked that question. One of our business-to-consumer side of the house is we're actually going to complement the common certifications—so, Security+, Certified Ethical Hacker, CISSP—where that gets to our problem that I previously mentioned that you'd get both Security+ and even Ethical Hackers that didn't actually know how to do a lot of stuff from a technical standpoint.

SHAWN MONSEN: Right.

JUSTIN PARKER: So, we're going to build in training paths for each one of those type of thing. So, Security+ go with the, for lack of a better term, syllabus for everything that somebody is going to be learning during Security+, and then coming up with micro-scenarios along the way that teach that skillset from a keyboard perspective, not just from a textbook perspective.

So, in short, the answer to your question is it's relatively easy. The hard part for us, which we have as a resource, is coming up with scenarios that are applicable and relevant to teach that skillset. With our heavy Cybersecurity presence and personnel, coming up with scenarios is actually very easy, but it also depends on the customer, too—do you have a scenario in your mind that you want us to do? And then it's sending back and forth. Or do you want to hand us a syllabus and say, "Hey, come up with scenarios that teach all these things along the way?" We're pretty flexible when it comes to that kind of stuff.

So, it's pretty easy. It usually takes us anywhere between a week to two weeks of dev time to come up with something, depending on the complexity of it. Sometimes it's even only a couple days. Then, like I said earlier, once you have the foundation there, it's even faster because we're literally just adding stuff on top of it. So, you can do those mini-tests along the way, or you can treat it like a sandbox environment where you're building on top of it as you go, or "Hey, I'm teaching one thing—OK, they've got that in there, and now I'm going to add something else to it as well and build upon that skillset in one particular range.

[00:53:23]

STEVE WRIGHT: You know, Justin, maybe I'm remembering that old movie, *The Last Starfighter*, but ***to what extent could students, not employees, use your range as part of a course and actually get customized training for a particular employer?***

The biggest challenge we have—and you went through those numbers in the beginning of how many jobs and how great this need is, but still there's this huge gap of getting people in the field and working with employers. Do you have anything in the works to help that happen?

[00:53:52]

JUSTIN PARKER: Yeah, I really appreciate you asking that question. We actually are working on that. From the business-to-consumer side of house, we're working on the badging thing. So, once they complete an entire skill path, they get a badge, and that badge is the… I can't remember the framework for it, but it's something they can put on their LinkedIn profile.

Our goal is to make Haiku an industry test block as well, that somebody can go through—a student or somebody that's looking for a job—and be able to demonstrate, in addition to "I have a Security+ certification," I've also demonstrated my skillset of going through the Haiku Security+ path, and I've been certified through that path, and here's my badge to show that I can do it.

So, that's our way of being able to advertise to employers. I mean, we're even looking at it as kind of a potential recruiting tool, and we've had recruiters talk to us as well of being able to say, "Hey, if somebody wants to be able to transmit their information to a recruiter of them demonstrating these skillsets by going through Haiku, can they sign up and do that?" Now, that's in further releases of our business-to-consumer, but it's definitely on our board as well.

[00:55:05]

STEVE WRIGHT: Yeah, we're seeing a number of business models where recruiters under different business concepts end up helping students pay for education in order to qualify for jobs that they're actually being retained to fill through enterprise or government agencies. So, to the extent that this becomes more complex, we need to understand how our students can participate, and it sounds like you might be beginning to look at that.

The key is to find out what it is that they really want the student to know because we're going in a world where, traditionally, people look for degrees, and now, increasingly, as you brought out, it's the skillsets. Now, obviously, the answer is a little bit of both, but in order for students without a degree to qualify for a job, they need to have a pretty precise fit on the skillset—could you elaborate on that?

[00:56:00]

JUSTIN PARKER: Yeah. So, I think that gets back to the challenge that we're running into right now, which is it's not well defined, right? We have these certifications that everybody agrees to—Security+, Network+, Certified Ethical Hacker, things like that as well. There's one out, and I apologize the name escapes me right now—that does require them to do hands-on demonstration, but that's a pretty high-up one, COSP? I apologize—I can't remember off the top of my head.

But I do agree with that challenge that we're having right now, which is, yeah, there's not currently a governing body that says, "Yes, this person not only understands the textbook side of the house, but they've been able to demonstrate that skillset as well," and we're trying to fill that gap by doing this type of product.

I've got some questions from Alex on this side of the house. I do know that we're a little over time. Nicole, this is your show—I'm happy to stay and answer questions as long as you guys need me to, but it's up to you.

[00:56:57]

NICOLE SHERMAN: Yes, please! That would be wonderful. Thank you.

[00:57:00]

JUSTIN PARKER: OK. Yeah, so is it possible to provide NVP product review...that came from Alex. I apologize—can you expand upon what NVP product review is a little bit more? Or what you mean by NVP? OK, all right, I'll do research and happily get back to you, Nicole, on that one. The badges—

[00:57:33]

ALEX: Hey, guys, I apologize.

JUSTIN PARKER: No, you're fine.

ALEX: Yeah, I'm here. I apologize. I just was seeking… It took me a second to get to the unmute button. Yeah, I guess, I'm a student at the American River Los Rios District Community College, and I believe this is kind of aimed at the community college's workforce development and faculty, and I think it's also focused for the students. And correct me if I'm wrong—is this the appropriate room for me to be in to discuss these topics?

[00:58:06]

STEVE WRIGHT: Yes, you're welcome.

ALEX: Thank you so much. Just some of the questions I had were… I come from the private sector. I guess I'm an entrepreneur/lifetime practitioner, and some of the things that I mentioned in the questions, real quick, are things that would be relevant to my peers, myself, as well as, I guess, employers—

[00:58:34]

JUSTIN PARKER: Alex, I don't know if you cut off there…

RICHARD GROTEGUT: I think Alex muted himself or somebody muted him.

JUSTIN PARKER: Yeah, like I said, I'll go real quick here. Workforce development CCC staff, specific programs, absolutely, that kind of gets them to the Enterprise Solution side of the house. We do internal workforce development with Haiku. If some kind of new policy mandate comes out or something like that as well, we, more often than not, spin up some kind of range to demonstrate that policy. We've had some discussions, although we haven't gotten all the way there with various state agencies on workforce development or workforce testing. I don't like to use the word 'testing' because sometimes when you deal with the union side of the house, that can get kind of in dangerous territory.

Badges recognized by governing industry bodies or associations, we're working on it. It doesn't exist right now. So, the idea is that if you bring it and have this solution and everybody agrees it's a good idea, then they become recognized, so it's kind of a grassroots approach to it. We are talking about partnering with some of the larger governing entities, like Security+ and things like that as well, but I think that they're looking for feedback once we go the business-to-consumer side of the house.

By the way, our business-to-consumer release 1 is scheduled to be out at the end of this year, if not beginning of next year. We're actually doing our beta testing on it right now, so I'll make sure that I let Nicole and Shawn and Steve be aware when the business-to-consumer release actually becomes live. You can actually go to HaikuRange.com and sign up to be notified as well.

Local enterprise technology, business partnerships—I think I just touched on that. And students test out to earn badges… Well, I mean, the test-out process is demonstrating to be able to go through the path very quickly. We're designing these paths that each micro-range takes about 20 minutes or less to go through if somebody already knows how to do everything. It's kind of like playing Legend of Zelda—if you know how to go everywhere, you're going to finish that game in a few hours. If you don't know what you're doing, you're going to spend days in there. So, that's kind of our test-out process that we're working with right now.

Martin's point—yes, that is an absolute challenge right now that I run into all the time. They want an entry-level person that has 2 to 3 years of background experience, and we're trying to tackle that with this as well, of being able to say, "Hey, they have a Security+, they have this, and this person can demonstrate that they do all that stuff."

Myself as an employer, I love bringing in no experience, by a corporate standpoint, employees that are all-stars and talents. What I'll tell you right now is, as I'm seeing folks… This demand is so crazy right now that once you get your foot in the door of the Cybersecurity mafia, for lack of a better term, after a couple years of experience, I'm having a hard time keeping these guys because folks are hiring them away at double their salary. It's crazy right now, and I know everybody is happy to see that.

But yeah, I think that the market is starting to warm up a little bit more towards having people with no actual corporate experience. I think that they're just looking for a solution that shows they know exactly what they're doing, and like I said, we're hoping that the Haiku Range can be one of those solutions.

[01:02:12]

STEVE WRIGHT: OK, I think we're going to wrap it up with that. This has been really informative, Justin, and for those of you who have people you know that might have enjoyed seeing this, this is recorded and will be posted on our website in about late next week, along with the transcript and the slide, so it's a real advantage for you to share.

We're going to skip next week, but we're going to come back on October 25 with how to save money on certifications with CompTIA's Academy Partner Program—that will be interesting to a lot of you. All right, well, Justin, thank you very much and everybody else for participating today. Have a good day.

JUSTIN PARKER: Thanks, folks. I appreciate it.

Additional Resources

- Visit www.ictdmsector.org for complete fall schedule and past webinars
- Go to HaikuRange.com and sign up to be notified about updates and releases